Exhibit R-2, RDT&E Budget Item Justification: PB 2012 Defense Advanced Research Projects Agency										DATE: February 2011	
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*				R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*							
COST ($ in Millions)	**FY 2010**	**FY 2011**	**FY 2012 Base**	**FY 2012 OCO**	**FY 2012 Total**	**FY 2013**	**FY 2014**	**FY 2015**	**FY 2016**	**Cost To Complete**	**Total Cost**
Total Program Element	271.316	281.262	400.499	-	400.499	368.621	378.741	397.164	411.831	Continuing	Continuing
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	92.131	100.791	91.732	-	91.732	70.633	65.400	61.092	59.092	Continuing	Continuing
IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*	109.140	126.930	208.419	-	208.419	195.659	195.385	196.491	196.491	Continuing	Continuing
IT-04: *LANGUAGE TRANSLATION*	70.045	53.541	67.015	-	67.015	52.329	51.289	56.248	56.248	Continuing	Continuing
IT-05: *CYBER TECHNOLOGY*	-	-	33.333	-	33.333	50.000	66.667	83.333	100.000	Continuing	Continuing

A. Mission Description and Budget Item Justification

The Information and Communications Technology program element is budgeted in the applied research budget activity because it is directed toward the application of advanced, innovative computing systems and communications technologies.

The High Productivity, High-Performance Responsive Architectures project is developing the necessary computing hardware and the associated software technology base required to support future critical national security needs for computationally-intensive and data-intensive applications. These technologies will lead to new multi-generation product lines of commercially viable, sustainable computing systems for a broad spectrum of scientific and engineering applications; it will include supercomputer, embedded computing systems, and novel design tools for manufacturing of defense systems.

The Information Assurance and Survivability project is developing the technology required to make emerging information system capabilities (such as wireless and mobile code/mobile systems) inherently secure, and to protect DoD's mission-critical systems against attack upon or through the supporting information infrastructure. These technologies will enable our critical systems to provide continuous correct operation even when they are attacked, and will lead to generations of stronger protection, higher performance, and more cost-effective security and survivability solutions scalable to several thousand sites.

The Language Translation project will develop and test powerful new Human Language Technology that will provide critical capabilities for a wide range of national security needs. This technology will enable systems to a) automatically translate and exploit large volumes of speech and text in multiple languages obtained through a variety of means; b) to have two-way (foreign-language-to-English and English-to-foreign-language) translation; c) enable automated transcription and translation of foreign speech and text along with content summarization; and d) enable exploitation of captured, foreign language hard-copy documents.

The Cyber Technology project supports long term national security requirements through the development and demonstration of technology to increase the security of military information systems. This involves networking, people, platforms, weapons sensors, and decision aids to create a whole that is greater than the sum of

Exhibit R-2, RDT&E Budget Item Justification: PB 2012 Defense Advanced Research Projects Agency	DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	**R-1 ITEM NOMENCLATURE** PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*

its parts. The results are networked forces that operate with increased speed and synchronization and are capable of achieving massed effects without the physical massing of forces as required in the past.

B. Program Change Summary ($ in Millions)	FY 2010	FY 2011	FY 2012 Base	FY 2012 OCO	FY 2012 Total
Previous President's Budget	272.191	281.262	279.383	-	279.383
Current President's Budget	271.316	281.262	400.499	-	400.499
Total Adjustments	-0.875	-	121.116	-	121.116
• Congressional General Reductions		-			
• Congressional Directed Reductions		-			
• Congressional Rescissions	-	-			
• Congressional Adds		-			
• Congressional Directed Transfers		-			
• Reprogrammings	6.345	-			
• SBIR/STTR Transfer	-7.220	-			
• TotalOtherAdjustments	-	-	121.116	-	121.116

Congressional Add Details ($ in Millions, and Includes General Reductions)	FY 2010	FY 2011
Project: IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*		
Congressional Add: *High Speed Optical Interconnects for Next Generation Supercomputing*	1.200	-
Congressional Add Subtotals for Project: IT-02	1.200	-
Project: IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*		
Congressional Add: *Intelligent Remote Sensing for Urban Warfare*	1.200	-
Congressional Add Subtotals for Project: IT-03	1.200	-
Congressional Add Totals for all Projects	2.400	-

Change Summary Explanation

FY 2010: Decrease reflects internal below threshold reprogramming offset by SBIR/STTR transfer.

FY 2012: Increase reflects expanded efforts in cyber related research and language translation offset by a reduction for Defense Efficiencies for contractor staff support.

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency			DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	

COST ($ in Millions)	FY 2010	FY 2011	FY 2012 Base	FY 2012 OCO	FY 2012 Total	FY 2013	FY 2014	FY 2015	FY 2016	Cost To Complete	Total Cost
IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*	92.131	100.791	91.732	-	91.732	70.633	65.400	61.092	59.092	Continuing	Continuing

A. Mission Description and Budget Item Justification

The High Productivity, High-Performance Responsive Architectures project is developing high-productivity, high-performance computer hardware and the associated software technology base required to support future critical national security needs for computationally-intensive and data-intensive applications. These technologies will lead to new multi-generation product lines of commercially viable, sustainable computing systems for a broad spectrum of scientific and engineering applications; it will include both supercomputer and embedded computing systems. One of the major challenges currently facing the DoD is the prohibitively high cost, time, and expertise required to build large complex software systems. Powerful new approaches and tools are needed to enable the rapid and efficient production of new software, including software that can be easily changed to address new requirements and can adjust dynamically to platform and environmental perturbations. The project will ensure accessibility and usability to a wide range of application developers, not just computational science experts. This project will also focus on novel design tools for the manufacture of complex ground and aerospace systems.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
Title: Architecture Aware Compiler Environment (AACE)	10.404	13.923	-

Description: The Architecture Aware Compiler Environment (AACE) program will develop computationally efficient compilers that incorporate learning and reasoning methods to drive compiler optimizations for a broad spectrum of computing system configurations. AACE compilers will greatly simplify application development by providing the capability to automatically and efficiently generate compiled code that effectively exercises the targeted computer system resources for computer systems that range from a single, multi-core processor system to very large, multi-processor systems. The AACE program will dramatically reduce application development costs and labor; ensure that executable code is optimal, correct, and timely; enable the full capabilities of computing system advances to our warfighters; and provide superior design and performance capabilities across a broad range of military and industrial applications.

FY 2010 Accomplishments:
- Developed and demonstrated initial system characterization tools.
- Performed compiler Preliminary Design Review (PDR).
- Created the initial common development environment and developed supporting technologies.
- Successfully met AACE Phase I goals and metrics, for transition into Phase II.

FY 2011 Plans:

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency		DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
- Complete characterization tools. - Perform research on compiler optimizations that utilize system characterization tools. - Develop runtime learning environment. - Create initial compiler environment and prototype. - Perform compiler Critical Design Review (CDR). - Demonstrate AACE Phase II goals and metrics.			
Title: META ***Description:*** The goal of the META program is to develop novel design flows, tools, and processes to enable a significant improvement in the ability to design complex defense and aerospace systems that are correct-by-construction. The program seeks to develop a design representation of meta-language and a domain-specific component model library from which system designs can quickly be assembled and their correctness verified with a high degree of certainty. Such a "fab-less" design approach is complemented by a foundry-style manufacturing capability, consisting of a factory capable of rapid reconfiguration between a large number of products and product variants through bitstream reprogramability, i.e., with minimal or no resultant learning curve effects. Together, the fab-less design and foundry-style manufacturing capability is anticipated to yield substantial---by a factor of five to ten---compression in the time to develop and field complex defense and aerospace systems. The META effort will also explore the initial design of a next generation ground combat vehicle by employing a novel, model-based correct-by-construction design capability, a highly-adaptable foundry-style manufacturing capability, and crowd-sourcing methods to demonstrate 5x-10x compression in the timeline necessary to build an infantry fighting vehicle. Beginning in FY 2012, the specific ground vehicle application work will be funded in PE 0602702E, Project TT-04, Advanced Land Systems. ***FY 2010 Accomplishments:*** - Began development of a new model-based systems engineering process, novel design, integration, and verification flows, and appropriate supporting metrics. - Began development of a meta-language for the representation of models of both software and physical system components. ***FY 2011 Plans:*** - Continue development of supporting tools necessary to implement the model-based design, integration, and verification flows. - Begin development of a foundry configuration toolset to enable the (re)configuration of foundry-style manufacturing capabilities for a given required degree of manufacturing adaptability. - Exercise feedback loop between manufacturability constraints and the system design toolset.	14.074	49.000	56.000

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency		DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
- Begin development and testing of crowd-sourced design infrastructure for electromechanical and software systems for a next generation ground combat vehicle. ***FY 2012 Plans:*** - Develop a domain-specific component model library for the military ground vehicle domain through extensive characterization of desirable and spurious interactions, dynamics, and properties of all constituent components down to the numbered part level. - Develop context models to reflect various operational environments. - Develop a domain-specific foundry configuration for military ground vehicles. - Begin the assembly and integration of foundry-style manufacturing capability for military ground vehicles. - Develop and implement an infrastructure for publishing and maintaining detailed component models using the metalanguage construct to expand the design space for subsequent efforts to design and build a military ground vehicle. - Develop a mechanism for the feedback of manufacturability constraints into the design and design tradespace exploration process. - Develop and integrate a library of various fabrication processes and associated manufacturing elements, i.e., machines and techniques employed to produce the various constituent elements of the military ground vehicle.			
Title: Ubiquitous High Performance Computing (UHPC)* ***Description:*** * Formerly Extreme Computing. The Ubiquitous High Performance Computing (UHPC) program is creating the technology base necessary for computing systems with performance that exceeds one quintillion operations per second. The UHPC program addresses some of the most challenging areas for embedded and supercomputer systems: power, programming and resiliency to faults/errors. The program is developing the specific technologies necessary for revolutionary improvements relative to scalable performance, productivity, physical size, power, programmability, dependability, data bandwidth, latency, and optimized data placement/storage. Within the context of DoD systems, mechanisms for self-modification and self-optimization will enable extreme computing systems to radically improve performance. This program will develop self-aware trusted computing techniques that will provide autonomous system monitoring. ***FY 2010 Accomplishments:*** - Initiated UHPC collaborative research environments. - Performed initial research on new execution models.	12.866	30.000	5.500

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency		DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
- Established preliminary design approaches for the UHPC systems. ***FY 2011 Plans:*** - Research and develop critical technologies, system methodologies, and architectures to enable general-purpose computing systems to achieve UHPC program goals. - Complete models of five UHPC challenge problems. - Develop initial simulations of critical technologies. ***FY 2012 Plans:*** - Initiate detailed system design with analyses and simulations including critical technology demonstrations. - Formulate approaches for achieving resiliency to faults and errors in high performance embedded computing systems.			
Title: Unconventional Warfighters ***Description:*** The Unconventional Warfighters program will create information technologies that enable new classes of participants to contribute to defense missions. One such class includes futurists, inventors, hobbyists, and tinkerers who approach military problems from an unconventional perspective. This latent source of creativity has been successfully tapped in the commercial sector through crowd-sourcing Internet marketplaces that bring human intelligence to bear on tasks for which computers are poorly suited. Information extraction and integration techniques will enable the solutions proposed by individuals to be correlated and fused into meta-solutions for further iterative development. Another class of potential participants is military Veterans, including disabled Veterans, who have deep knowledge of the missions and the operational environment. Machine learning tools will enable individuals with similar interests and complementary capabilities to find each other while advanced collaboration tools will amplify the synergies of diverse dynamic groups. Animals are another class of potential contributors. This is not a new idea, as animals possessing special abilities such as dogs and dolphins have been used before to perform military tasks such as mine detection. The new aspect to be examined under Unconventional Warfighters is the potential for creating new sensor, processing, communication and actuator systems specially adapted to enable animals to execute tasks beyond their natural capabilities. ***FY 2012 Plans:*** - Conceptualize and develop tools to enable persons with similar interests and complementary capabilities to find each other and collaborate on military problems. - Develop techniques for correlating and fusing solution concepts put forward by diverse proposers to yield "meta-solutions" for complex military problems.	-	-	25.000

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency		DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
- Design and develop sensor, processing, communication and actuator systems specially adapted to enable animals to execute tasks beyond their natural capabilities.			
Title: High-Productivity Computing Systems (HPCS) ***Description:*** The HPCS program will create a new generation of economically viable, high-productivity computing systems for the national security and industrial user communities. HPCS technologies will enable nuclear stockpile stewardship, weapons design, cryptanalysis, weather prediction, and other large-scale problems that cannot be addressed productively with today's computers. The goal of this multi-agency program is to develop revolutionary, flexible and well-balanced computer architectures that will deliver high performance with significantly improved productivity for a broad spectrum of applications. Additionally, programming such large systems will be made easier so engineers and scientists can better harness the power of high-performance computers. ***FY 2010 Accomplishments:*** - Incorporated HPCS interconnect technology in a supercomputer product line and delivered to a DoD customer. - Fabricated and tested a terabits-per-second hub chip that will enable the first petascale system with global shared memory. - Successfully demonstrated a high-performance prototype system that can be scaled up to become the world's fastest and most capable supercomputer. ***FY 2011 Plans:*** - Complete the Phase III prototypes and demonstrate that they meet their goals of world-leading performance and productivity. - Demonstrate Unified Parallel C performance improvements in symmetric multiprocessing, distributed and hybrid modes. - Provide the HPCS stakeholders with access to the prototype systems for a six-month evaluation and experimentation period. ***FY 2012 Plans:*** - Complete demonstration of prototype systems with stakeholders.	51.933	7.868	5.232
Title: Software Producibility ***Description:*** A variety of new processor and systems architectures, including multicore and stream processors, large-scale virtualization, and the cloud computing paradigms are becoming the norm for both military and civilian computing infrastructure. Unfortunately, these are highly complex technologies that exceed the capabilities of most of our programmers/application developers, and the result is that the cost of software is skyrocketing. The Software Producibility program addressed this critical issue by creating technologies that reduce the cost, time, and expertise required to build large complex software systems, while ensuring that security and service guarantees are met.	1.654	-	-

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency		DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	**R-1 ITEM NOMENCLATURE** PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	**PROJECT** IT-02: *HIGH PRODUCTIVITY, HIGH-PERFORMANCE RESPONSIVE ARCHITECTURES*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
One promising approach is an intelligent software development system that learns specific implementations of a number of high-level designs, and then uses this knowledge to create initial implementations of novel high-level designs. Automating the development of initial implementations, and then expanding this intelligence to automate debugging will save the software developer considerable time and effort. ***FY 2010 Accomplishments:*** - Conducted load-time field update experiments. - Conducted preliminary design-time security adaptation experiments. - Conducted run-time adaptation and online run-time reconfiguration experiments. - Explored candidate demonstration systems, in addition to those used by the performer that will foster transition to the Services. - Created initial strategies for software frameworks to support multi-core, stream, and cloud computing.			
Accomplishments/Planned Programs Subtotals	90.931	100.791	91.732

	FY 2010	FY 2011
Congressional Add: High Speed Optical Interconnects for Next Generation Supercomputing	1.200	-
FY 2010 Accomplishments: - Initiate research into High Speed Optical Interconnects for Next Generation Supercomputing.		
Congressional Adds Subtotals	1.200	-

C. Other Program Funding Summary ($ in Millions)

N/A

D. Acquisition Strategy

N/A

E. Performance Metrics

Specific programmatic performance metrics are listed above in the program accomplishments and plans section.

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency			DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*	

COST ($ in Millions)	FY 2010	FY 2011	FY 2012 Base	FY 2012 OCO	FY 2012 Total	FY 2013	FY 2014	FY 2015	FY 2016	Cost To Complete	Total Cost
IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*	109.140	126.930	208.419	-	208.419	195.659	195.385	196.491	196.491	Continuing	Continuing

A. Mission Description and Budget Item Justification

The Information Assurance and Survivability project is developing the core computing and networking technologies required to protect DoD's information, information infrastructure, and mission-critical information systems. These technologies will enable DoD information systems to operate correctly and continuously even when they are attacked, and will provide cost-effective security and survivability solutions. Technologies developed under this project will benefit other projects within this program element as well as projects in the Command, Control, and Communications program element (PE 0603760E), the Network-Centric Warfare Technology program element (PE 0603764E), the Sensor Technology program element (PE 0603767E), and other projects that require secure, survivable, network-centric information systems.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
Title: Cyber Genome	8.500	13.000	24.000
Description: The Cyber Genome program will develop break-through cyber-forensic techniques to characterize, analyze, and identify malicious code. This will allow for the automatic discovery, identification, and characterization of any future variants of previously unknown malicious code in computing systems. Cyber Genome will also develop break-through abilities in visualization, threat identification analysis, and threat mitigation analysis to enable positive identification of malicious code substructures and functionality. ***FY 2010 Accomplishments:*** - Developed automatic techniques to rapidly and interactively reconstruct metadata to assist in the analysis of potentially malicious code. - Refined technologies, ontologies, and algorithms to enable the characterization of future malicious code variants based on analyzed malicious code substructures. - Established teams, instituted community training, and generated test data sets to evaluate the malicious code detection techniques. ***FY 2011 Plans:*** - Expand and refine technologies, ontologies, and algorithms to enable the characterization of future malicious code variants based on analyzed malicious code substructures. - Complete integration of automatic discovery, identification, analysis, and prediction algorithms.			

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency		DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
- Refine user signature identification model and correlate with physical security methods. ***FY 2012 Plans:*** - Continue Cyber Genome prototype experiments. - Create lineage trees for a class of digital artifacts to gain a better understanding of software evolution. - Generate execution trees from submitted malware that include automated analysis of software dependencies. - Identify and/or validate DoD users from their host and/or network behavior. - Commence transition of Cyber Genome prototype to a transition partner.			
Title: Integrity Reliability Integrated CircuitS (IRIS)* ***Description:*** *Formerly DISCOVER The Department of Defense has become increasingly reliant on electronic parts and systems fabricated outside of the United States. In many cases, these parts have also been designed in foreign countries, and there is currently no method available to decipher the full functionality of these circuits that may contain billions of transistors. Even if the part is designed domestically, there is currently no way of verifying that no tampering has occurred during fabrication, especially as processing technology scales to near atomic length scales, that can compromise the warfighter's mission or safety. Integrity Reliability Integrated CircuitS (IRIS) will advance non-destructive reverse engineering of integrated circuits whose functionality is not known a priori. These tools will be compatible with leading edge 32 nanometer complementary metal-oxide semiconductor (CMOS) node size. These tools will ensure that an integrated circuits' full functionality is known and will provide verification that no malicious changes have been introduced. ***FY 2010 Accomplishments:*** - Commenced definition of functional requirements for algorithms that determine circuit functionality without full knowledge of their underlying logic and design. ***FY 2011 Plans:*** - Complete definition of functional requirements for algorithms that determine circuit functionality without knowledge of their underlying logic and design. - Design tools for non-destructive interrogation of integrated circuit functionality without prior knowledge of the designed functionality. ***FY 2012 Plans:*** - Demonstrate functional derivation of un-altered digital and mixed-signal circuits at 45 nm integrated circuit (IC) node. - Demonstrate reliability derivation from reduced sample sizes.	10.000	22.878	30.000

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency		DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
- Develop non-destructive techniques for reverse engineering a digital IC.			
Title: Trusted Software* ***Description:*** * Formerly Total Software Understanding (TSU) The Trusted Software program will meet DoD demands for reliable and robust software using technology to diagnose software for inefficiencies, design errors, redundant code, and overall software inconsistencies. Current software projects are massive, dynamic social efforts involving distributed teams of developers, marketers, and users. Without the proper tools, the software engineers create errors and redundancies providing unintended and exploitable security flaws. This program will develop specific techniques to extract information on software products, model the development environment, and integrate the models into low-level software analysis tools to provide a robust diagnostic tool for building and validating trustworthy software. ***FY 2011 Plans:*** - Develop a database of legacy software products that could contain exploitable flaws. - Initiate the design of software development models. ***FY 2012 Plans:*** - Prototype software development modeling environment. - Compare, for selected software platforms, actual software behavior against intended behavior. - Analyze and determine causes of differences between actual and intended software behavior.	-	5.000	10.000
Title: Agile Assured Computing * ***Description:*** * Previously Confident Computing The Agile Assured Computing program will radically change the current paradigm of overly complex, unwieldy, and insecure computing platforms. Current commercial off-the-shelf platforms add layer upon layer of functionality and have become hugely complex and difficult to maintain. The current approach to securing these platforms emphasizes large security applications, such as anti-virus programs, that in themselves are difficult to maintain and vulnerable to attack. The Agile Assured Computing program will create more flexible, responsive methods for securing computing systems that operate in challenging environments. The program will develop automated system technologies to identify and mitigate vulnerabilities in legacy computing platforms. Agile Assured Computing technologies will reduce security risk without requiring lengthy development cycles or time-consuming maintenance by system administrators. ***FY 2011 Plans:***	-	5.349	10.000

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency		DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
- Identify mechanisms to determine outdated and unnecessary system attributes used for attacks. - Initiate development of automated tools for identifying system attributes for attacks. - Identify approaches for modifying those attributes to provide a secure operating pathway. ***FY 2012 Plans:*** - Demonstrate mechanisms to determine outdated and unnecessary system attributes used for attacks. - Demonstrate automated tools for identifying system attributes for attacks. - Demonstrate approaches for modifying those attributes to provide a secure operating pathway.			
Title: Rapid Planning (RP) ***Description:*** The Rapid Planning (RP) program will develop rapid planning and replanning tools based on recent mathematical advances such as topological data analysis (TDA). The program will develop tools and techniques for rapid generation and adaptation of robust plans in the presence of uncertainty, imprecision, incomplete, and contradictory data and assumptions. RP will also provide a capability for monitoring plans, providing continuous replanning capability, and plain text explanations for recommended plans. RP will invest in mathematical methods to improve optimization including new branch and bound, mixed integer programming, and sub-modularity methods; techniques for accelerated simulation where accuracy can be traded for speed; design of experiments through manifold learning and identification techniques that build upon previous DARPA programs; and develop a process that is aware of interdependencies in plans and aids planners in resolving these interdependencies. ***FY 2011 Plans:*** - Create overarching system architecture for rapid replanning incorporating environmental and tactical uncertainty. - Design automated identification of the controlling and nuisance parameters to quickly focus attention. - Implement TDA techniques to predict optimal performance in an evolving non-linear environment. ***FY 2012 Plans:*** - Develop techniques for rapidly assessing the robustness of plans and create the ability for planners to quickly develop and deploy plan contingencies to address potential failure modes. - Demonstrate and assess the efficacy of the tool to rapidly create and adapt plans more accurately in a military laboratory environment.	-	5.000	9.169
Title: Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH)* ***Description:*** *Formerly Cyber Immune	-	15.000	29.000

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency		DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
The Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH) program will develop cyber security technologies using the mechanisms of biological systems as inspiration for radically re-thinking basic hardware and system designs. Higher level organisms have two distinct immune systems: the innate system is fast and deadly but is only effective against a fixed set of pathogens; the adaptive system is slower, but can learn to recognize novel pathogens. Similarly, CRASH will develop mechanisms at the hardware and operating system level that eliminate known vulnerabilities exploited by attackers. However, because novel attacks will be developed, CRASH will also develop software techniques that allow it to defend itself, to maintain its capabilities, and even heal itself. Finally, biological systems show that diversity is an effective population defense; CRASH will develop techniques that make each computer system appear unique to the attacker and allows each system to change over time. ***FY 2011 Plans:*** - Develop initial designs of one or more systems, including novel hardware and system features. - Demonstrate through formal methods, simulation, and design walkthroughs that the prototype systems mitigate common technical vulnerabilities. ***FY 2012 Plans:*** - Integrate and implement one or more CRASH hardware systems capable of supporting the prototype operating system. - Demonstrate the ability to detect and recover from penetrations. - Red-team systems to verify technical vulnerabilities known by the community have been addressed successfully.			
Title: Safer Warfighter Computing (SAFER)* ***Description:*** *Formerly Securing the Hosts The Safer Warfighter Computing (SAFER) program is creating a technology base for assured and trustworthy Internet communications and computation, particularly in untrustworthy and adversarial environments. SAFER creates automated processes and technologies that will enable military users to send and receive content on the Internet, utilizing commercially available hardware and software, in ways that avoid efforts to deny, locate, or corrupt communications. SAFER is also developing technology for performing computations on encrypted data without decrypting it first through fully homomorphic encryption and interactive, secure multi-party computation schemes. This will enable, for example, the capability to encrypt queries and to create an encrypted search result without decrypting the query. This technology will advance the ability to run computationally intensive programs on large datasets on a cluster of untrusted computers, as in a cloud computing environment, while keeping programs, data, and results encrypted and confidential. ***FY 2011 Plans:*** - Develop technical approaches for improving the security of internet-based communications and computation.	-	13.275	20.000

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency		DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
- Demonstrate initial security and availability capabilities. - Demonstrate initial encryption algorithms and measurement capabilities. - Demonstrate the feasibility of homomorphic encryption. ***FY 2012 Plans:*** - Demonstrate robust security and availability capabilities. - Demonstrate robust encryption algorithms and measurement capabilities.			
Title: Anomaly Detection at Multiple Scales (ADAMS)* ***Description:*** *Formerly part of Security-Aware Systems The Anomaly Detection at Multiple Scales (ADAMS) program will develop and apply algorithms for detecting anomalous behaviors over multiple scales of space and time. Spatially, ADAMS technologies will apply to systems, individuals, groups/organizations, and nation-states. Temporally, ADAMS technologies will apply to behaviors that emerge over hours, days, months, and years. ADAMS will develop flexible, scalable and highly interactive approaches to extracting actionable information from information system log files, sensors, and other instrumentation as needed. ***FY 2011 Plans:*** - Conceptualize approaches for finding indicators of anomalous behaviors buried in enormous amounts of observational data. ***FY 2012 Plans:*** - Create a scalable, distributed architecture to collect, store, access, process, and correlate relevant data from heterogeneous sources over extended periods of time. - Formulate techniques for determining whether a system, individual, group/organization, or nation-state is exhibiting anomalous behavior suggestive of an emerging threat.	-	4.500	18.000
Title: Cyber Reserve Corps ***Description:*** The Cyber Reserve Corps program will develop technologies and tools to enable and educate private citizens to participate in the defense of cyberspace. Private citizens already collaborate on cyber-defense through the numerous blogs and message boards dedicated to issues such as diagnosing problems on home computers/networks and remediating the effects of malware on popular commercial systems. These activities are facilitated through a variety of software tools; additional tools for detecting and diagnosing known exploits and variants of known exploits will be developed. Cyber Reserve Corps will also create technologies for generating shareable host and network log files that are both informative with respect to new exploits yet preserve the privacy of user data, as well as tools for automating the analysis of these log files. Ordinarily this information would	-	-	20.000

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency		DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
remain widely distributed, but Cyber Reserve Corps will make it possible to bring it all together to reveal subtle patterns of hostile activity that would otherwise go unnoticed. ***FY 2012 Plans:*** - Develop concepts for collaborative cyber-defense encompassing public and private hosts/networks. - Develop technologies that enable confidential sharing of detailed host data and configuration information. - Develop techniques for sensing widely distributed probes/attacks on public/private networks.			
Title: Resilient Networks ***Description:*** The Resilient Networks program will create technologies that enable networks to survive cyber attack. Many vulnerabilities have been identified in the networking protocols used in the routers and switches used in home/small business, enterprise, and wide-area networks. While attackers are able to adapt their attacks in a highly dynamic fashion, the capability to respond to such attacks is limited by the complexity of the networking protocols and their typically proprietary, vendor-specific implementations. Resilient Networks will address this by creating advanced routing/switching software that runs efficiently on commodity processors. Such software-defined routers/switches will enable far greater agility in responding to exploits than is presently possible and provide the basis for highly reactive networked defense capabilities. Resilient Networks will also address embedded computing systems such as vehicle/platform/weapon/industrial control systems, which must operate at a high level of assurance in real-world environments. Resilient Networks will develop new verification and validation techniques for embedded networks that must function reliably in complex adversarial environments. Achieving resilience in enterprise networks is also of interest. This would involve techniques for reconfiguring enterprise networking and computing resources to mitigate the effects of attacks and restore services. ***FY 2012 Plans:*** - Recast datalink and network layer protocols for parallel execution on commercial multicore processors. - Design high-utilization protocol primitives for implementation in widely used development environments while respecting multi-level security requirements. - Perform an in-depth systems engineering analysis to identify changes required to enable simplified provisioning of secure communications and networking services. - Identify algorithmic advances and protocol re-design opportunities/needs to achieve high levels of assurance in internet-based wide-area communications/networking and in embedded networked computing and control systems. - Develop and apply new algorithms and protocols in high-assurance implementations for use in wide-area communications/ networking and in embedded networked computing and control systems.	-	-	20.000
Title: Assured Mobile Platform (AMP)	-	-	18.250

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency		DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
Description: The Assured Mobile Platform (AMP) program will develop and demonstrate the technologies required to secure wireless mobile devices. As in the civilian world, the military is making increasing use of wireless devices such as smartphones and personal digital assistants. These devices integrate computational and wireless networking elements that are controlled by a so-called "mobile platform". The mobile platform integrates a computer operating system with software for controlling the wireless component. Because mobile devices have very limited size, weight, and power, the mobile platform must be very efficient and so can devote only a limited share of its computational resources to security. This makes securing mobile wireless devices a challenge. Cross-layer approaches are extremely promising due to the emergence of low-cost electronically-steerable antenna arrays suitable for mobile devices. Another approach is to utilize off-board security resources accessed via the cloud, in effect "security reach-back". AMP will develop, mature, and integrate these technologies to produce a mobile platform that provides a high level of assurance for military users. ***FY 2012 Plans:*** - Explore cross-layer approaches for securing mobile platforms that incorporate an electronically-steerable antenna array. - Formulate "security reach-back" approaches that utilize off-board security resources to secure mobile platforms. - Perform detailed requirements analysis and systems engineering as the basis for a concept of operations and high level design for a mobile platform that provides a high level of assurance for military users.			
Title: Next Generation Core Optical Networks (CORONET) ***Description:*** The Next Generation Core Optical Networks (CORONET) program will revolutionize the operation, performance, security, and survivability of the United States' critical inter-networking system by leveraging technology developed in DARPA photonics component and secure networking programs. These goals will be accomplished through a transformation in fundamental networking concepts that form the foundation upon which future inter-networking hardware, architecture, protocols and applications will be built. Key technical enablers that will be developed in this thrust include: 1) network management tools that guarantee optimization of high density wavelength-division-multiplexed (WDM) optical channels; 2) creation of a new class of protocols that permit the cross-layer communications needed to support quality-of-service requirements of high-priority national defense applications; and 3) demonstration of novel concepts in applications such as distributed and network-based command and control, intelligence analysis, predictive logistics management, simulation- and scenario-enhanced decision-making support for real-time combat operations, and assured operation of critical U.S. networking functions when faced with severe physical layer attack. These network-based functions will support the real-time, fast-reaction operations of senior leadership, major commands and field units. ***FY 2010 Accomplishments:*** Next-Generation Core Optical Networks (CORONET)	16.069	12.785	-

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency		DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
- Worked with DISA to ensure that CORONET's next phase incorporates the requirements and technology evolution plan of their DISN-Core network. - Initiated the CORONET next phase development of network control and management software and associated test plan such that the final product will be suitable for transition and implementation in current and future commercial and DoD core optical networks. Transmission, Switching and Applications for CORONET - Completed a feasibility study of high-spectral efficiency banded WDM fiber-optic transmission system. ***FY 2011 Plans:*** Next-Generation Core Optical Networks (CORONET) - Continue the CORONET next phase effort to develop the network control and management software, the CORONET network-emulation testbed and the plans for technical testing and demonstrations, and formulate the technology transition plan. - Continue to work with DISA on technical oversight and evaluation of the CORONET software development effort and associated test plan. - Engage Standards Bodies, with the appropriate endorsements of both DISA and the commercial carrier members of the CORONET team, with the goal of amending the existing standards with the developed CORONET technology. - Pursue opportunities for commercial transition as well as future integration into the DISN-Core and other DoD networks.			
Title: Intrinsically Assured Mobile Ad-Hoc Networks (IAMANET) ***Description:*** The Intrinsically Assured Mobile Ad-Hoc Network (IAMANET) program continues a series of successful research programs to design a tactical wireless network that is secure and resilient to a broad range of threats which include cyber attacks, electronic warfare and malicious insiders (or captured/compromised radios). Previous programs included the Dynamic Quarantine of Computer-Based Worms (DQW) and Defense Against Cyber Attacks on Mobile Ad-hoc Network Systems (DCAMANET). IAMANET will build upon the successes achieved in both the DQW and the DCMANET programs. IAMANET directly supports the integrity, availability, reliability, confidentiality, and safety of Mobile Ad-hoc Network (MANET) communications and data. In contrast, the dominant Internet paradigm is intrinsically insecure. For example, the Internet does not deny unauthorized traffic by default and therefore violates the principle of least privilege. In addition, there are no provisions for non-repudiation or accountability and therefore adversaries can probe for vulnerabilities with impunity because the likelihood of attributing bad behavior to an adversary is limited. Current protocols are not robust to purposely induced failures and malicious behavior, leaving entire Internet-based systems vulnerable in the case of defensive failure. IAMANET, on the other hand, uses a deny-by-default networking paradigm, allowing only identifiable authorized users to communicate on the network. While the objective transition	14.543	11.912	-

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency		DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
path for IAMANET technologies is to the Services to support mobile tactical operations, the IAMANET systems are interoperable with fixed networks and may also have potential applicability to the broader DoD network architecture. ***FY 2010 Accomplishments:*** - Completed the assessment of technologies developed for possible integration into MANET's. - Transitioned the IAMANET technologies to the Military Networking Protocol (MNP) program for developing robust user authentication and attribution. - Initiated the design, development and integration of a secondary subsystem for the Microsoft Windows XP platform. - Initiated design and proof of concept development of trusted hardware components. - Conducted evaluation in simulated operational networks at the United States Military Academy. ***FY 2011 Plans:*** - Complete the design, development and integration of a secondary subsystem for the Microsoft Windows XP platform. - Complete design and proof of concept development of trusted hardware components. - Integrate technologies into DoD's existing information assurance desktop security application Host Based Security Suite (HBSS) to enable widespread deployment.			
Title: Trustworthy Systems ***Description:*** The goal of the Trustworthy Systems program is to provide new approaches to network-based monitoring that provide maximum coverage of the network (i.e. from the NIPRNET/Internet gateway to service enclaves) with performance independent of the network's size, and with computational costs that either remain constant or decrease as the network's speed or relative size increases. The end deliverable of this program will provide network defense technologies with: (1) high probability of detection (Pd) of malicious traffic per attack launched and, (2) a false alarm rate of not more than one false alarm per day. This technology will provide gateway-and-below network traffic monitoring approaches that scale at rates that are linear (or less) to increases in network size and transmission speeds. ***FY 2010 Accomplishments:*** - Constructed a unique testing environment that supports network speeds in excess of 40 Gbps. - Completed initial asymmetric routing pathway flow and traffic analysis algorithms and initiated integration into Commercial-of-the-Shelf (COTS) high speed switching device. - Completed initial testing of the prototype intrusion detection system at 1 Gbps on an Application Services Gateway hardware system. ***FY 2011 Plans:*** - Develop and integrate test-case scenarios to be used in final product testing.	13.090	7.731	-

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency		DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
- Complete final asymmetric routing pathway flow and traffic analysis algorithms and initiate integration into COTS high speed switching device to meet 40 Gbps speed thresholds. - Perform network testing of the 10 Gbps and 40 Gbps products.			
Title: Security-Aware Systems ***Description:*** The Security-Aware Systems program developed and advanced a variety of potentially promising technologies to enable the military to field secure, survivable, self-monitoring, self-defending network centric systems. This program evaluated security aware systems that will avoid brittleness and vulnerability, due to their ability to reason about their own security attributes, capabilities and functions with respect to specific mission needs. These systems also dynamically adapt to provide desired levels of service while minimizing risk and providing coherent explanations of the relative safety of service level alternatives. The systems bolster the reliability and security of critical software systems by reducing vulnerabilities and logic errors, and providing state-of-the-art software analysis techniques augmented with cognitive decision-making techniques. Research efforts also explored provable protection of information and investigate technologies that enable fundamentally new approaches for detecting insider threats. ***FY 2010 Accomplishments:*** - Investigated the application of Self-Regenerative Systems (SRS) technology to a high value, mission critical, military computing system. - Examined the ability of SRS technology to enable a military computing system to successfully complete a mission in the face of cyber attack or accidental fault.	5.397	-	-
Title: Cyber Insider Threat* ***Description:*** *Formerly part of Security-Aware Systems The Cyber Insider Threat (CINDER) program will develop techniques for countering one of the most significant and malicious threats to military networks and systems: the cyber insider threat. Current defenses are based on network and host intrusion detection, and look for "break-ins" and abnormal behavior but do not attempt to characterize a user's mission. The CINDER program will build tools and techniques that characterize user mission in a multi-level security environment. These concepts and technology will continue in PE 0603760E, Project CCC-04 beginning in FY 2012. ***FY 2010 Accomplishments:*** - Obtained realistic exemplars of insider threat activities. ***FY 2011 Plans:***	5.000	10.500	-

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency		DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-03: *INFORMATION ASSURANCE AND SURVIVABILITY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
- Use machine learning to develop rule-based models of user behavior. - Identify and characterize templates for adversary class, mission and stage of existing compromises for insider threat activities.			
Title: Trusted, Uncompromised Semiconductor Technology (TrUST) ***Description:*** The Trusted, Uncompromised Semiconductor Technology (TrUST) program addressed the fundamental problem of determining whether a microchip manufactured through a process that is inherently "untrusted" (i.e., not under our control) can be "trusted" to perform operations only as specified by the design, and no more. The program consisted of a set of complementary technologies integrated together which developed a product that transitioned to the DoD. ***FY 2010 Accomplishments:*** - Protected Field Programmable Gate Arrays (FPGAs) from unauthorized substitutions to improve and empirically verify the software/firmware framework for using Physically Unclonable Functions. - Integrated a TrUSTed IC solution for Application Specific Integrated Circuits (ASICs) and FPGAs that are ready for transition. - Developed advanced non-destructive IC reverse engineering techniques. - Identified, developed, and quantified performance of innovative destructive and non-destructive evaluation techniques for ICs at the 45 nm node.	35.341	-	-
Accomplishments/Planned Programs Subtotals	107.940	126.930	208.419

	FY 2010	FY 2011
Congressional Add: Intelligent Remote Sensing for Urban Warfare ***FY 2010 Accomplishments:*** - Conducted research in remote sensing for urban warfare operations.	1.200	-
Congressional Adds Subtotals	1.200	-

C. Other Program Funding Summary ($ in Millions)

N/A

D. Acquisition Strategy

N/A

E. Performance Metrics

Specific programmatic performance metrics are listed above in the program accomplishments and plans section.

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency			DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-04: *LANGUAGE TRANSLATION*	

COST ($ in Millions)	FY 2010	FY 2011	FY 2012 Base	FY 2012 OCO	FY 2012 Total	FY 2013	FY 2014	FY 2015	FY 2016	Cost To Complete	Total Cost
IT-04: *LANGUAGE TRANSLATION*	70.045	53.541	67.015	-	67.015	52.329	51.289	56.248	56.248	Continuing	Continuing

A. Mission Description and Budget Item Justification

This project is developing powerful new technologies for processing foreign languages that will provide critical capabilities for a wide range of military and national security needs, both tactical and strategic. The technologies and systems developed in this project will enable our military to automatically translate and exploit large volumes of speech and text in multiple languages obtained through a variety of means.

Current U.S. military operations involve close contact with a wide range of cultures and peoples. The warfighter on the ground needs hand-held, speech-to-speech translation systems that enable communication with the local population during tactical missions. Thus, tactical applications imply the need for two-way (foreign-language-to-English and English-to-foreign-language) translation.

Because foreign-language news broadcasts, web-posted content, and captured foreign-language hard-copy documents can provide insights regarding local and regional events, attitudes and activities, language translation systems also contribute to the development of good strategic intelligence. Such applications require one-way (foreign-language-to-English) translation. Exploitation of the resulting translated content requires the capability to automatically collate, filter, synthesize, summarize, and present relevant information in timely and relevant forms.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
Title: Global Autonomous Language Exploitation (GALE)	38.353	22.945	11.250
Description: The Global Autonomous Language Exploitation (GALE) program will create an integrated product enabling automated transcription and translation of foreign speech and text with targeted information retrieval. When applied to foreign language broadcast media and web-posted content, GALE systems will enhance open-source intelligence and local/regional situational awareness by reducing the cost and effort of translation and analysis. GALE will produce a fully-mature architecture and dramatically improve transcription and translation accuracy by broader exploitation of context. GALE will develop timely alerts for commanders and warfighters. ***FY 2010 Accomplishments:*** - Exercised language-independent paradigm for new languages essential for military use - Dari, Pashto and Urdu. - Developed methods for porting targeted information retrieval technology into new languages. - Developed methods for using extraction-empowered machine translation, in which the system extracts the meaningful phrases (e.g., names and descriptions) from foreign language text for highly accurate translation into English.			

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency		DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-04: *LANGUAGE TRANSLATION*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
- Completed the architecture for a summarization system that incorporates adaptive filtering, focused summarization, information extraction, contradiction detection, and user modeling. ***FY 2011 Plans:*** - Achieve high accuracy translation and distillation using shallow semantics with minimal ancillary information. - Achieve translation accuracy and distillation that exceeds human performance. - Provide technology updates to military and intelligence operations centers. ***FY 2012 Plans:*** - Incorporate the sophisticated search capabilities developed in the distillation task of GALE into the inserted systems. - Transition to new customers.			
Title: Multilingual Automatic Document Classification, Analysis and Translation (MADCAT) ***Description:*** The Multilingual Automatic Document Classification, Analysis and Translation (MADCAT) program will develop and integrate technology to enable exploitation of captured, foreign language, hand-written documents. This technology is crucial to the warfighter, as documents including notebooks, letters, ledgers, annotated maps, newspapers, newsletters, leaflets, pictures of graffiti, and document images captured in the field may contain extremely important time-sensitive information. The MADCAT program will address this need by producing devices that will convert such captured documents from Arabic into readable English in the field. MADCAT will substantially improve applicable technologies, in particular document analysis and optical character recognition/optical handwriting recognition. MADCAT will tightly integrate these improved technologies with translation technology and create prototypes for field trials. ***FY 2010 Accomplishments:*** - Developed algorithms for interpreting different regions within a document; removing noise from contaminated and degraded documents; predicting the syntactic structure and propositional content of text; and extracting information from an address field or the axes of a table. - Integrated these technologies with the translation and summarization components of GALE to yield tightly integrated technology prototypes that convert captured documents into readable and searchable English. ***FY 2011 Plans:*** - Complete the development of algorithms for interpreting different regions within a document; for predicting the syntactic structure and propositional content of text; and for removing noise from contaminated and degraded documents. - Complete the integration of these improvements with the translation and summarization components of GALE. - Transition tightly integrated technology prototypes that convert captured documents into readable and searchable English to high-impact military systems and intelligence operations centers.	14.663	15.375	19.870

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency		DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-04: *LANGUAGE TRANSLATION*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
- Develop language independent technology extensions to Dari, Pashto and Urdu. - Train and test the technology on data collected in the field. - Develop a system that handles with both handwritten and machine-printed text. ***FY 2012 Plans:*** - Continue to improve translation accuracy. - Continue development of language independent and script independent technology. - Continue training and testing of field collected data. - Continue training and testing of documents containing printed and hand-written text. - Transition tightly integrated technology prototypes to military and intelligence operations centers.			
Title: Robust Automatic Translation of Speech (RATS) ***Description:*** The Robust Automatic Translation of Speech (RATS) program will address noisy and hostile conditions where speech signals are degraded by distortion, reverberation, and/or competing conversation. Robust speech processing technologies will enable soldiers to hear or read clear English versions of what is being said in their vicinity, despite a noisy or reverberant environment. RATS technology will isolate and deliver pertinent information to the warfighter by detecting periods of speech activity and discarding silent portions, determining the language spoken, identifying the speaker, and recognizing key words in challenging environments. ***FY 2010 Accomplishments:*** - Developed noise suppression and speech exploitation approaches based on multi-microphone arrays. - Started refinement of new speech processing techniques for noisy environments, including echo suppression, speech activity detection, language identification, speaker identification and keyword spotting. ***FY 2011 Plans:*** - Optimize new speech processing techniques for noisy environments, including speech activity detection, language identification, speaker identification and keyword spotting. - Develop bio-inspired algorithms to enable RATS processing. - Develop methods for detecting relevant speech segments. - Adapt present technologies for automatic speech recognition systems to cope with highly degraded signals. - Transition tightly integrated technology prototypes to military and intelligence operations centers. ***FY 2012 Plans:*** - Continue to improve processing techniques for noisy environments, including speech activity detection, language identification, speaker identification and keyword spotting.	9.196	12.721	20.895

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency		DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-04: *LANGUAGE TRANSLATION*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
- Train system on field collected data and test system in realistic environments. - Continue to work with transition partners.			
Title: Boundless Operational Language Translation (BOLT) ***Description:*** The Boundless Operational Language Translation (BOLT) program will enable communication regardless of medium (voice or text), and genre (conversation, chat, or messaging) through expansion of language translation capabilities, human-machine multimodal dialogue, and language generation. The BOLT program will enable warfighters and military/government personnel to readily communicate with coalition partners and local populations and will enhance intelligence through better exploitation of all language sources including messaging and conversations. The program will also enable sophisticated search of stored language information and analysis of the information by increasing the capability of machines for deep language comprehension. ***FY 2012 Plans:*** - Formulate approaches for automatically processing informal genres, interpreting poor pronunciation, coping with incorrect/ incomplete syntax, resolving references, and correlating co-references. - Conceptualize approaches for comprehension of colloquialisms and idiomatic speech. - Enable machines to carry on multi-modal dialogues with humans and to comprehend concepts and generate responses in multilingual environments.	-	-	15.000
Title: Spoken Language Communication and Translation System for Tactical Use (TRANSTAC) ***Description:*** The Spoken Language Communication and Translation System for Tactical Use (TRANSTAC) program is developing technologies that enable robust, spontaneous, two-way tactical speech communications between our warfighters and native speakers. The program addresses the issues surrounding the rapid deployment of new languages, especially low-resource languages and dialects. TRANSTAC is building upon existing speech translation platforms to create a rapidly deployable language tool that will meet the military's language translation needs. TRANSTAC is currently focusing on key languages of the Middle East region. ***FY 2010 Accomplishments:*** - Tested and refined the Dari prototype. - Developed context management translation techniques. - Demonstrated a hands-free, eyes-free, two-way translator prototype. - Extended translation techniques to develop translation systems emphasizing other key languages such as Pashto. ***FY 2011 Plans:***	7.833	2.500	-

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency		DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-04: *LANGUAGE TRANSLATION*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
- Develop simultaneous multi-lingual translation techniques. - Demonstrate a multilingual translation prototype. - Test translation systems emphasizing other key languages.			
Accomplishments/Planned Programs Subtotals	70.045	53.541	67.015

C. Other Program Funding Summary ($ in Millions)

N/A

D. Acquisition Strategy

N/A

E. Performance Metrics

Specific programmatic performance metrics are listed above in the program accomplishments and plans section.

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency			DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-05: *CYBER TECHNOLOGY*	

COST ($ in Millions)	FY 2010	FY 2011	FY 2012 Base	FY 2012 OCO	FY 2012 Total	FY 2013	FY 2014	FY 2015	FY 2016	Cost To Complete	Total Cost
IT-05: *CYBER TECHNOLOGY*	-	-	33.333	-	33.333	50.000	66.667	83.333	100.000	Continuing	Continuing

A. Mission Description and Budget Item Justification

The Cyber Technology project supports long term national security requirements through the development and demonstration of technology to increase the security of military information systems. Over the past decade the DoD has embraced net-centric warfare to enable geographically dispersed forces to attain a high level of shared battlespace awareness that is exploited to achieve strategic, operational, and tactical objectives. This involves networking people, platforms, weapons, sensors, and decision aids to create a whole that is greater than the sum of its parts. The results are networked forces that operate with increased speed and synchronization and are capable of achieving massed effects without the physical massing of forces as required in the past. Adversaries seek to limit this "force multiplier" effect through cyber attacks intended to degrade, disrupt, or deny military computing, communications, and networking systems. Due to its importance and the emergence of these threats, cyberspace is now recognized as a critical warfighting domain, equal in importance to the more traditional domains of sea, air, land, and space. Technologies developed under the Cyber Technology project will ensure DoD cyber-capabilities survive adversary cyber attacks. Promising technologies will transition to system-level projects.

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
Title: Cyber Situational Awareness and Response (CSAR)	-	-	17.500
Description: The Cyber Situational Awareness and Response (CSAR) program will develop technologies to enable awareness and understanding of the cyber environment as required for decision making for defensive and/or responsive actions. This includes attack detection, characterization, and assessment, attacker identification, and information/system provenance. Cyber situational awareness is made increasingly difficult by efforts of attackers to elude detection. Approaches to cyber situational awareness will include techniques to exploit data derived from events on hosts and networks that may be quite subtle when examined in isolation but more apparent when correlated in time and space across an enterprise. CSAR will also create new graphical interfaces and Web 2.0 mashups that enable intuitive visualization of anomalous events on hosts and networks suggestive of cyber attack. Toward this end, CSAR will develop, apply and assess pattern detection and analysis and machine learning techniques to create a real-time network forensics capability that can serve as the basis for rapid response capabilities including network reconstitution. This is an area where metrics are difficult to obtain and so CSAR will extend operationally-meaningful measures such as mean-time-to-detect and false-alarm rate to estimate the efficacy of schemes proposed to detect important classes of attacks. ***FY 2012 Plans:*** - Identify events on hosts and networks having the greatest potential to provide indications and warning of cyber attack. - Conceptualize new graphical interfaces that enable intuitive visualization of anomalous events on hosts and networks suggestive of cyber attack.			

Exhibit R-2A, RDT&E Project Justification: PB 2012 Defense Advanced Research Projects Agency		DATE: February 2011
APPROPRIATION/BUDGET ACTIVITY 0400: *Research, Development, Test & Evaluation, Defense-Wide* BA 2: *Applied Research*	R-1 ITEM NOMENCLATURE PE 0602303E: *INFORMATION & COMMUNICATIONS TECHNOLOGY*	PROJECT IT-05: *CYBER TECHNOLOGY*

B. Accomplishments/Planned Programs ($ in Millions)	FY 2010	FY 2011	FY 2012
- Develop canonical classes of cyber attacks and operationally-meaningful metrics to estimate the efficacy of cyber situational awareness and response schemes.			
Title: Cyber Camouflage, Concealment, and Deception (C3D) ***Description:*** The Cyber Camouflage, Concealment, and Deception (C3D) project will develop novel approaches for protecting cyber systems that mimic camouflage concealment, and deception in the physical world. C3D will enable the creation, deployment, management, and control of synthetic entities, objects, resources, and identities that create uncertainties for attackers and make their task significantly more difficult, perhaps even intractable. With C3D, infrastructure and other enterprise resources such as switches, servers, and storage could be virtually replicated to confound enemy targeting. Multiple C3D copies of file systems, only one of which holds correct information, will require attackers (including insiders) to either exfiltrate many times the data they would normally (and then work to identify which data is correct) or to guess which file system contains operationally meaningful data, thereby greatly decreasing their odds for success. Ultimately, C3D will produce intelligent artificial users that can defeat phishing attacks. C3D will make attackers work harder and take more risks to achieve their goals and will enhance the effectiveness of conventional cyber defenses. ***FY 2012 Plans:*** - Develop a framework for the creation, deployment, management, and control of synthetic entities, objects, resources, and identities on enterprise information systems. - Develop approaches for creating multiple plausible versions of file systems and data where provenance will be uncertain for the attacker. - Explore techniques capable of deceiving an attacker into believing they have executed a successful phishing attack when in fact they have been deceived by an intelligent synthetic user.	-	-	15.833
Accomplishments/Planned Programs Subtotals	-	-	33.333

C. Other Program Funding Summary ($ in Millions)

N/A

D. Acquisition Strategy

N/A

E. Performance Metrics

Specific programmatic performance metrics are listed above in the program accomplishments and plans section.